UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,239	01/23/2006	Thomas Fountain	200634-0109-00-US (425596	9717

23973 7590 03/30/2009

DRINKER BIDDLE & REATH
ATTN: INTELLECTUAL PROPERTY GROUP
ONE LOGAN SQUARE
18TH AND CHERRY STREETS
PHILADELPHIA, PA 19103-6996

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/30/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/519,239	FOUNTAIN ET AL.	
	Examiner	Art Unit	
	SHIN-HON CHEN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-64* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-64* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :12/22/04, 1/17/06, 1/23/06, and 4/7/08.

DETAILED ACTION

1. Claims 1-64 have been examined.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 12/22/04, 1/17/06, 1/23/06 and 4/7/08 are being considered by the examiner.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-64 are rejected under 35 U.S.C. 102(b) as being anticipated by Spies et al. U.S. Pat. No. 5689565 (hereinafter Spies).

6. As per claim 1, Spies discloses a cryptographic key server suitable for providing cryptographic services to remote devices coupled to said cryptographic key server via a network, said cryptographic key server comprising:

a secure network interface engine executing on said cryptographic key server, said secure network interface engine operable: to establish a secure network communication channel with at

least one remote device (Spies: column 3 lines 17-31: the cryptographic application program interface);

to unmarshal secured cryptographic service requests received from said at least one remote device (Spies: column 5 lines 7-18: communications are secure); and

to marshal and transmit secure cryptographic service responses to said at least one remote device (Spies: column 5 lines 7-18: secure exchange of document); and

a cryptographic service engine executing on said cryptographic key server, said cryptographic service engine being in bi-directional communication with said secure network interface engine, said cryptographic service engine operable to provide cryptographic services requested by said at least one remote device via said secure network interface engine (Spies: column 3 lines 17-34).

7. As per claim 2, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses wherein said at least one device is an application server (Spies: column 5 lines 35-44).

8. As per claim 3, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses wherein said secure network interface engine is arranged such that said secure network communication channel is established according to a Secure Socket Layer (SSL) protocol (Spies: column 5 lines 7-11).

9. As per claim 4, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses wherein said secure network interface engine is arranged such that said secure network communication channel is established according to a Transport Layer Security (TLS) protocol (Spies: column 5 lines 7-11).

10. As per claim 5, Spies discloses cryptographic key server as recited in claim 1. Spies further discloses wherein said secure network interface engine supports multiple communications protocols including a Secure Socket Layer (SSL) protocol and a Transport Layer Security (TLS) protocol, said secure network interface engine being responsive to said at least one device to establish said secure network communication channel according to a protocol selected by said at least one device (Spies: column 5 lines 20-44).

11. As per claim 6, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses wherein said cryptographic service engine and said secure network interface engine are components of a single process executing on said cryptographic key server (Spies: column 3 lines 6-16).

12. As per claim 7, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses wherein said cryptographic service engine is operable to perform encryption and decryption functions (Spies: column 3 lines 18-19).

13. As per claim 8, Spies discloses the cryptographic key server as recited in claim 7. Spies further discloses wherein said encryption and decryption functions comprise: symmetric block ciphers; generic cipher modes; stream cipher modes; public-key cryptography; padding schemes for public-key systems; key agreement schemes; elliptic curve cryptography; one-way hash functions; message authentication codes; cipher constructions based on hash functions; pseudo random number generators; password based key derivation functions; Shamir's secret sharing scheme and Rabin's information dispersal algorithm (IDA); DEFLATE (RFC 1951) compression/decompression with gzip (RFC 1952) and zlib (RFC 1950) format support; fast multi-precision integer (bignum) and polynomial operations; finite field arithmetic, including GF(p) and GF(2.sup.n); and prime number generation and verification (Spies: column 3 lines 17-20: different cryptographic functions).

14. As per claim 9, Spies discloses the cryptographic key server as recited in claim 7. Spies further discloses wherein said encryption and decryption functions comprise: DES, 3DES, AES, RSA, DSA, ECC, RC6, MARS, Twofish, Serpent, CAST-256, DESX, RC2, RC5, Blowfish, Diamond2, TEA, SAFER, 3-WAY, Gost, SHARK, CAST-128, Square, Shipjack, ECB, CBC, CTS, CFB, OFB, counter mode(CTR), Panama, ARC4, SEAL, WAKE, Wake-OFB, Blumblumshub, ElGamal, Nyberg-Rueppel (NR), Rabin, Rabin-Williams (RW), LUC, LUCELG, DLIES (variants of DHAES), ESIGN padding schemes for public-key systems: PKCS#1 v2.0, OAEP, PS SR, IEE P1363 EMSA2, Diffie-Hellman (DH), Unified Diffie-Hellman (DH2), Menezes-Qu-Vanstone (MQV), LUCDIF, XTR-DH, ECDSA, ECNR, ECIES, ECDH, ECMQV, SHA1, MD2, MD4, MD5, HAVAL, RIPEMD-160, Tiger, SHA-2 (SHA-256,

SHA-384, and SHA-512), Panama, MD5-MAC, HMAC, XOR-MAC, CBC-MAC, DMAC, Luby-Rackoff, MDC, ANSI X9.17 appendix C, PGP's RandPool, PBKDF1 and PBKDF2 from PKCS #5 (Spies: column 3 lines 17-20: various cryptographic functions not limited to the above mentioned algorithms).

15. As per claim 10, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses wherein said cryptographic service engine is operable to perform signing and verifying functions (Spies: column 3 lines 18-19).

16. As per claim 11, Spies discloses the cryptographic key server as recited in claim 10. Spies further discloses wherein said signing and verifying operations includes RSA and DSA (Spies: column 8 lines 49-60).

17. As per claim 12, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses wherein said cryptographic service engine is operable to perform hashing operations (Spies: column 10 lines 50-54).

18. As per claim 13, Spies discloses the cryptographic key server as recited in claim 10. Spies further discloses wherein said hashing operations includes HMAC with SHA-1 (Spies: column 22 lines 64-67).

19. As per claim 14, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses wherein said cryptographic service engine is further operable to authenticate and to determine authorization of a request for cryptographic services prior to and as a condition of performing said cryptographic services (Spies: column 6 lines 44-59).

20. As per claim 15, Spies discloses the cryptographic key server as recited in claim 14. Spies further discloses wherein authenticating a request for cryptographic services includes verifying an identity of one or more of a set comprising: a client that is requesting for cryptographic services; said at least one remote device from which said client requesting for cryptographic services; a function or program that is executing on said at least one remote device (Spies: column 21 lines 21-61: verification).

21. As per claim 16, Spies discloses the cryptographic key server as recited in claim 14. Spies further discloses wherein determining authorization of a request for cryptographic services includes determining authorization privileges granted to one or more of a set comprising: a client that is requesting for cryptographic services; said at least one remote device from which said client requesting for cryptographic services; a function or program that is executing on said at least one remote device (Spies: column 3 lines 19-32).

22. As per claim 17, Spies discloses the cryptographic key server as recited in claim 16. Spies further discloses wherein the operation of determining authorization a request for cryptographic services further includes determining whether said request for cryptographic

services is within the privileges of a requestor that is associated with said request for cryptographic services (Spies: column 7 lines 1-16).

23. As per claim 18, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses wherein said cryptographic service engine is operable to track requests for cryptographic services (Spies: column 3 lines 49-61).

24. As per claim 19, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses said cryptographic key server further comprising: a private key engine, said private key engine operable to provide private keys for use by said cryptographic service engine in performing cryptographic services (Spies: column 3 lines 37-48).

25. As per claim 20, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses wherein said cryptographic key server is a network security appliance (Spies: column 3 lines 6-16).

26. As per claim 21, Spies discloses the cryptographic key server as recited in claim 1. Spies further discloses wherein said cryptographic key server has a computer hardware architecture supporting said cryptographic service engine and said secure network interface engine, said computer hardware architecture comprising: a databus; a central processing unit bi-directionally coupled to said databus; a persistent storage device bi-directionally coupled to said databus; a transient storage device bi-directionally coupled to said databus; a network I/O device bi-

directionally coupled to said databus; a cryptographic accelerator card bi-directionally coupled to said databus; a hardware security module bi-directionally coupled to said databus and suitable for storing private keys; and a smart card interface device (Spies: figure 11 and column 17 lines 1- 58).

27. As per claim 22, Spies discloses the cryptographic key server as recited in claim 21. Spies further discloses wherein said hardware security module is a tamper resistant device (Spies: column 3 lines 37-49).

28. As per claim 23, Spies discloses the cryptographic key server as recited in claim 21. Spies further discloses wherein said private keys are loaded into said hardware security module and stored in an encrypted format (Spies: column 3 lines 37-49).

29. As per claim 24, Spies discloses the cryptographic key server as recited in claim 21. Spies further discloses wherein said private keys are loaded into said hardware security module via a smart card storing said encrypted private keys (Spies: column 19 lines 9-17).

30. As per claim 25, Spies discloses the cryptographic key server as recited in claim 24. Spies further discloses wherein said cryptographic key server supports a k-out-of-n secret sharing such that said private keys may only be accessed by said cryptographic key server after k smart cards have been inserted (Spies: column 19 lines 9-18).

31. As per claim 26-64, claims 16-64 encompass the same scope as claims 1-25. Therefore, claims 26-64 are rejected based on the same reason set forth above in rejecting claims 1-25.

Conclusion

32. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Dickinson et al. U.S. Pat. No. 7187771 discloses server-side implementation of a cryptographic system.

Cross et al. U.S. Pub. No. 20040146015 discloses deriving a symmetric key from an asymmetric key for file encryption or decryption.

Cromer et al. U.S. Pub. No. 20020129261 discloses method for encrypting and decrypting data recorded on portable cryptographic tokens.

Koved et al. U.S. Pat. No. 7308717 discloses method for supporting digital rights management in an enhanced java runtime environment.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIN-HON CHEN whose telephone number is (571)272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2431

/Shin-Hon Chen/
Examiner, Art Unit 2431